UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

RAH-NITA BOYKIN, individually and on behalf of all others similarly situated, Plaintiff, v. AT&T, INC., Defendant.	Case No.: 1:24-cv-02973 JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Rah-Nita Boykin ("Plaintiff") on behalf of herself and all others similarly situated, by and through her attorneys, brings this action against AT&T, INC. ("AT&T" or "Defendant") and alleges, upon her personal knowledge and as to her own actions and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Corporations that collect consumers' sensitive information, including their names, phone numbers, addresses, email addresses, dates of birth, financial account numbers, Social Security numbers and/or passport numbers ("Personally Identifiable Information" or "PII"), have a duty to the consumers to protect their valuable, sensitive information.

2. Defendant is one of the nation's largest telecommunications providers, selling cellular services and internet to both businesses and individual customers. As a corporation whose everyday course of business requires the gathering of highly sensitive consumer information in order to provide services, Defendant is well aware of the life-altering impact a data breach can have on the average AT&T customer.

3. Despite this knowledge, Defendant failed to properly protect customers by investing in adequate data security, thereby allowing hackers to exfiltrate the highly sensitive PII that customers entrusted to Defendant. In approximately mid-March 2024, Defendant became aware of a catastrophic, widespread data breach in which the data of at least 73 million current and former customers was breached and exfiltrated (the "Data Breach"). Most alarming, reports indicate that the data at issue may have originated from a 2021 data breach.[1]

4. On March 30, 2024, Defendant posted a notice to its website announcing that the sensitive information of more than 73 million current and former AT&T customers had been "released on the dark web approximately two weeks ago."[2] Specifically, "the data set appears to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders."[3]

5. Defendant later reported that highly sensitive PII was accessed and exfiltrated by hackers, including full names, email addresses, mailing addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers and passcodes. For impacted current customers, Defendant was required to reset account passcodes.

6. Despite Defendant's statement that it "take[s] cybersecurity very seriously and privacy is a fundamental commitment at AT&T,"[4] Defendant inexplicably failed to implement and maintain reasonable and adequate security procedures and practices to safeguard the PII of Plaintiff and the Class. Defendant currently maintains that "the source of the data is still being assessed."[5]

---

[1] https://www.scmagazine.com/news/att-confirms-theft-of-73m-records-7-6m-current-customers-affected (last accessed April 9, 2024).
[2] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed April 9, 2024).
[3] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed April 9, 2024).
[4] *See* Ex. A, Notice.
[5] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed April 9,

7. Early reports indicate that the data implicated in the Data Breach was stolen in 2021, meaning that Defendant has acted recklessly in ignoring a massive security violation for nearly three years. The size of the Data Breach and information Defendant has disclosed about the breach to date, including the age of the data, the need to hire external cybersecurity experts, and the sensitive nature of the impacted data, collectively demonstrate Defendant failed to implement reasonable measures to prevent the Data Breach and the exposure of highly sensitive customer information.

8. Defendant knew or should have known of the serious risk of harm caused by a data breach, including the importance of acting swiftly to protect PII. Yet, Defendant ignored reports of the Data Breach in 2021, only confirming the exfiltration in mid-March 2024, and waited more than two weeks after that to begin notifying individuals impacted by the Data Breach on March 30, 2024.

9. Defendant's failure to promptly notify Plaintiff and Class members that their PII was implicated due to Defendant's security failures virtually ensured that the unauthorized third parties who exploited Defendant's security vulnerabilities could monetize, misuse, and/or disseminate that PII before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated even beyond the Data Breach itself.

10. Plaintiff and Class members had a reasonable expectation and understanding that Defendant would adopt adequate data security safeguards to protect their PII.

11. However, Defendant failed to: take sufficient and reasonable measures to safeguard

---

2024).

its data security systems and protect highly sensitive data to prevent the Data Breach from occurring; to disclose to current and former customers the material fact that it lacked appropriate data systems and security practices to secure PII; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Because of Defendant's failures, Plaintiff and Class members suffered substantial harm and injury.

12. As a direct result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common law obligations, Plaintiff's and Class members' PII was accessed and acquired by unauthorized third parties for the purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of Defendant's current and former customers.

13. Plaintiff and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

14. Plaintiff and Class members suffered injuries as a result of Defendant's conduct, including, but not limited to: lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to, the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct, and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on

their accounts; and the continued and increased risk of compromise to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect its PII. These risks will remain for the lifetimes of Plaintiff and the Class.

15. Plaintiff brings this action individually and on behalf of the Class, seeking relief including, but not limited to, compensatory damages, statutory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorneys' fees and costs, and all other remedies this Court deems proper.

II. PARTIES

16. Plaintiff Boykin is and has been at all relevant times a citizen and resident of Country Club Hills, Illinois.

17. Defendant AT&T, Inc. is a corporation organized under the state laws of Delaware with its headquarters and principal place of business located at 208 S. Akard St. Dallas, TX 75202.

III. JURISDICTION

18. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of costs and interest. At least one member of the Class is a citizen of a different state than Defendant, and there are more than 100 putative Class members.

19. Venue is proper in this judicial district under 28 U.S.C. § 1391 because Defendant transacts substantial business in this district, and because a substantial portion of the events giving rise to Plaintiff's claims occurred here.

20. This Court has personal jurisdiction over Defendant by virtue of its transactions and business conducted in this judicial district. For example, AT&T maintains a corporate office

in Chicago located at 225 W. Randolph St., Suite 2950, Chicago, IL 60606 where executive level employees such as a President, AT&T Illinois, run Defendant's Illinois operations.[6] Additionally, Defendant has dozens of branches in Illinois, where it employs retail sales consultants and retail managers, including, but not limited to, branches in West Loop, Lincoln Park, Bridgeport, and Irving Park, in Chicago, Illinois, and multiple Chicago-area suburban branches including Addison, Plainfield, Naperville, and Oswego.[7] Defendant has transacted and done business, and violated statutory and common law, in the State of Illinois and in this judicial district.

IV. FACTUAL BACKGROUND

A. Background

21. Defendant is one of the largest providers of telecommunications and technology services worldwide.

22. As relevant here, Defendant is the leading provider of mobile services in the United States (U.S.) with a market share of about 46.9 percent of wireless subscriptions in the third quarter of 2023.[8]

23. In 2023, Defendant generated $122.4 billion in revenue.[9]

24. Plaintiff and Class Members purchased cellular phone services from AT&T. As part of service enrollment, Defendant collected some of their most sensitive and confidential information, including, without limitation: name, email address, username, password, passcode,

[6] *See, e.g.,* https://www.attconnects.com/connecting-illinois-to-greater-possibility/ (last accessed April 9, 2024).

[7] *See, e.g.,* https://www.att.com/stores/illinois (last accessed April 9, 2024).

[8] https://www.statista.com/statistics/199359/market-share-of-wireless-carriers-in-the-us-by-subscriptions/ (last accessed April 9, 2024).

[9] https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/quarterly-earnings/2023/4q-2023/ATT_4Q_2023_8_K_Earnings_8_01.pdf (last accessed April 9, 2024).

Social Security number, account number, phone number, mailing address, financial information, and other personal and highly sensitive information a person might provide to receive cellular services.

25. As a result, Defendant hosts a large repository of sensitive personal information maintained for its customers and received from customers, including Plaintiff and the Class.

26. Defendant's Privacy Policy (the "Privacy Policy") is accessible on its website and clearly states: "We work hard to safeguard your information using technology controls and organizational controls. We protect our computer storage and network equipment. We require employees to authenticate themselves to access sensitive data. We limit access to personal information to the people who need access for their jobs. And we require callers and online users to authenticate themselves before we provide account information."[10]

27. Ironically, Defendant's Privacy Policy maintains that it collects PII in order to "[i]mprove your experience and safety. This includes verifying your identity, detecting and preventing fraud, protecting your financial accounts, authorizing transactions and assisting your interactions with customer care."[11]

28. Based on these policies and representations, Defendant owed Plaintiff and the Class a duty to protect their privacy and safeguard the sensitive personal information and PII of its current and former customers.

B. The Data Breach

29. Sometime in mid-March 2024, AT&T became aware that the details of 73 million former and current AT&T customer accounts, including full names, email addresses, mailing

[10] https://about.att.com/privacy/privacy-notice.html (last accessed April 9, 2024).

[11] https://about.att.com/privacy/privacy-notice.html (last accessed April 9, 2024).

addresses, phone numbers, dates of birth, social security numbers, AT&T account numbers and passcodes were "released on the dark web."[12]

30. Implicated data is presumed to be from 2019 or earlier, impacting approximately 7.6 million current AT&T account holders and approximately 65.4 million former account holders.[13]

31. In a later notice to impacted customers, AT&T revealed that highly sensitive PII was accessed and exfiltrated by hackers, including full names, email addresses, mailing addresses, phone numbers, social security numbers, dates of birth, AT&T account numbers and passcodes.[14] As a result, defendant was required to reset the passcodes of impacted customers.[15]

32. Although AT&T stated that it is currently unaware of how or when the data set was accessed, reports indicate that the Data Breach occurred sometime in 2021. Specifically, "[d]etails of the leaked data first appeared online in August 2021, when a known threat actor, ShinyHunters, offered up the records for sale on a hacking forum, with a 'buy it now' price of one million dollars."[16]

33. Now, the stolen data has been made nearly free on a dark web marketplace.[17] "Experts say the AT&T customer data sold online is legitimate and warn it could be used to launch

---

[12] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed April 9, 2024).

[13] https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html (last accessed April 9, 2024).

[14] *See* Ex. A.

[15] *Id.*

[16] https://tech.co/news/att-accounts-leaked-70-million-check (last accessed April 9, 2024).

[17] https://www.jimgogarty.com/tech-and-cybersecurity-a-closer-look-at-this-weeks-news-24-03-2024/#:~:text=The%20details%20of%20the%20leaked,another%20threat%20actor%2C%20Major%20Nelson. (last accessed April 9, 2024).

targeted attacks on those affected."[18]

34. As evidenced by availability of Plaintiff's and the Class members' data on the dark web, malicious actors accessed and acquired substantial amounts of Plaintiff's and the Class's sensitive personal information, including their PII. This data included highly sensitive personal information such as names, addresses, passcodes, and Social Security numbers.

C. Defendant's Failures Prior to and Following the Data Breach

35. Defendant knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

36. In fact, Defendant is no stranger to the risks posed by storing customer data because it suffered a third-party vendor breach in January 2023 that exposed nine million customer records.[19] Later in May 2023, a security researcher also disclosed a vulnerability that had allowed anyone with a target ZIP code and phone number to perform an account takeover via the AT&T website.[20]

37. Although it's unclear if the Data Breach was a ransomware attack, cyber-attacks and ransomware attacks are frequently used to target companies due to the volume of sensitive data that they collect, maintain, and store.[21] From 2022 to 2023, statistics show more than a 73%

[18] https://www.jimgogarty.com/tech-and-cybersecurity-a-closer-look-at-this-weeks-news-24-03-2024/#:~:text=The%20details%20of%20the%20leaked,another%20threat%20actor%2C%20Major%20Nelson. (last accessed April 9, 2024).

[19] https://www.cpomagazine.com/cyber-security/att-data-leak-73-million-account-passcodes-from-prior-to-2020-exposed-including-7-million-current-account-holders/ (last accessed April 9, 2024).

[20] https://www.cpomagazine.com/cyber-security/att-data-leak-73-million-account-passcodes-from-prior-to-2020-exposed-including-7-million-current-account-holders/ (last accessed April 9, 2024).

[21] Charles Griffiths, *The Latest 2023 Cyber Crime Statistics (updated October 2023)*, AAG (Feb. 10, 2023).

increase[22] in ransomware attacks, resulting in more than $1.1 billion in ransomware payments.[23]

38. According to the Center for Internet Security, companies should treat ransomware attacks as any other data breach incident because ransomware attacks do not simply hold networks hostage and/or publicly disclose the data; rather, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[24]

39. Defendant could have prevented this Data Breach by properly encrypting or otherwise protecting its equipment and network files containing PII.

40. Despite widespread industry warnings, Defendant failed to implement and use reasonable security procedures and practices to protect Plaintiff's and similarly situated individuals' sensitive PII.

41. Defendant's failure to properly safeguard Plaintiff's and Class members' PII allowed unauthorized actors to access this highly sensitive PII.

42. The Data Breach highlights the inadequacies inherent in Defendant's network monitoring procedures and security training protocols. If Defendant had properly monitored its cybersecurity systems and implemented a sufficient training protocol for its employees, it would have prevented the Data Breach, detected the Data Breach sooner, and/or have prevented the hackers from accessing PII.

43. Moreover, Defendant has not yet informed affected individuals of the length of time

---

[22] https://www.sans.org/blog/ransomware-cases-increased-greatly-in-2023/ (last accessed March 31, 2024).

[23] https://www.chainalysis.com/blog/ransomware-2024/ (last accessed March 31, 2024).

[24] *Ransomware: The Data Exfiltration and Double Extortion Trends*, Center for Internet Security, *available at* https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last accessed Apr. 12, 2024).

that the unauthorized actors had access to their PII, when the breach occurred, or the full extent of the PII that was accessed during the Data Breach.

44. Defendant's failure to timely notify Plaintiff and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

45. Defendant's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

46. Defendant's failures are three-fold. First, Defendant failed to timely secure its computer systems to protect its current and former customers' PII. Defendant allowed unauthorized actors to extract 73 million customer records without detection, and as a result, Plaintiff's and the Class's PII is currently available for sale on the dark web.

47. Second, Defendant failed to timely notify affected individuals, including Plaintiff and Class members, that their highly sensitive PII had been accessed by unauthorized third parties. At worst, AT&T knew of the Data Breach as early as 2021 but failed to take any action for ***more than three years***. At best, despite knowing that customer PII had been released on the dark web in mid-March 2024, Defendant waited approximately two weeks until March 30, 2024, to begin providing notice to the victims of the Data Breach.

48. Third, Defendant made no effort to protect Plaintiff and the Class from the long-term consequences of Defendant's acts and omissions. Although AT&T offered victims credit monitoring, Plaintiff's and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long into the future. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

49. In short, Defendant's myriad failures, including the failure to timely detect the Data

Breach and to notify Plaintiff and the Class with reasonable timeliness that their PII had been accessed due to Defendant's security failures, allowed unauthorized individuals to access and misappropriate Plaintiff's and Class members' PII for an unknown amount of time before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats to Consumers

50. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors and lead to considerable costs to consumers. According to Statista, during the first quarter of 2023 alone, more than six million data records were exposed worldwide through data breaches.[25] Indeed, cybercrime is slated to cost the world $10.5 trillion annually by 2025.[26]

51. Identity theft is the most common consequence of data breaches to consumers. A 2021 report concluded that more than half of all data breaches resulted in identity theft, including unauthorized access to a victim's financial accounts, opening new accounts in the victim's name, and using a victim's personal information for other fraudulent activities.[27]

52. As a result, consumers' PII is an invaluable commodity and the most frequent target of hackers.[28] Numerous sources cite dark web pricing for personal information, such as name, date of birth, and Social Security number, ranging from $40 to $200.[29]

---

[25] https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/ (last accessed April 9, 2024).

[26] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, Cybercrime Magazine (Nov. 13, 2020).

[27] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019).

[28] *Id*.

[29] *Id*.

53. Many tend to minimize the value of certain categories of PII, such as names, birthdates, addresses, and phone numbers. However, security experts agree that "[i]f you have someone's name and address, that is still valuable."[30] At the end of the day, "the more info you have, the more it is worth."[31]

54. Thefts of Social Security numbers present an even greater risk to consumers. Indeed, data breaches involving Social Security numbers are "incredibly alarming" because "[u]nlike a credit card number which can be changed, Social Security numbers . . . are hard to change, or cannot be changed."[32]

55. Even if victims whose Social Security numbers have been compromised are able to change their Social Security numbers, the new number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[33]

56. As relevant here, passcodes can lead to further incidents of identity theft. "A de-encrypted passcode plus the contact information that was found in the data leak (which includes names, addresses and birthdates) could very well be enough to pull off a SIM swap attack over the phone."[34]

57. In talking about the Data Breach, one cybersecurity specialist said "the combination

[30] Robert Lemos, *All about your 'fullz' and how hackers turn your personal data into dollars*, PCWorld (June 2, 2016).

[31] *Id.*

[32] Brian Naylor, *Victims Of Social Security Number Theft Find It's Hard To Bounce Back*, NPR (Feb. 9, 2015).

[33] *Id.*

[34] https://www.cpomagazine.com/cyber-security/att-data-leak-73-million-account-passcodes-from-prior-to-2020-exposed-including-7-million-current-account-holders/ (last accessed April 10, 2024).

of information in this breach and the overall size makes it more serious than usual."[35] Continuing on, she noted: "[t]he severity of this data breach is significantly heightened because of the Personal Identifiable Information (PII), including full names, email addresses, mailing addresses, phone numbers, Social Security numbers, dates of birth, AT&T account numbers and passcodes, that were part of the compromised data. The immediate concern is the potential exploitation of this exposed data, which could lead to various malicious activities such as identity theft, phishing attacks and unauthorized access to user accounts."

58. According to the FTC, in 2021, around 20% of Americans were victims of identity theft, indicating that most Americans have either been a victim of identity theft or know someone who has.[36]

59. The fraudulent activity resulting from Defendant's Data Breach may not come to light for years, as there may be a time lag between when Plaintiff's and Class members' PII was stolen and when it is used, meaning there may be a delay between when the harm occurs versus when it is discovered.[37]

60. Beyond economic impacts, identity theft also leads to lasting emotional impacts; a majority of the victims of identity theft report increased stress levels, fatigue, and trust issues with family and friends and decreased energy.[38]

---

[35] https://www.cpomagazine.com/cyber-security/att-data-leak-73-million-account-passcodes-from-prior-to-2020-exposed-including-7-million-current-account-holders/ (last accessed April 9, 2024).

[36] *Consumer Sentinel Network Data Book 2021*, Federal Trade Commission (Feb. 2022) *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf (last accessed April 10, 2024).

[37] *Report to Congressional Requesters*, Government Accountability Office, at 29 (June 2007) *available at* https://www.gao.gov/assets/gao-07-737.pdf (last accessed April 10, 2024).

[38] *New Study by Identity Theft Resource Center Explores the Non-Economic Negative Impacts Caused by Identity Theft*, Identity Theft Resource Center (Oct. 18, 2018).

61. Given the nature of Defendant's Data Breach, as well as the delay in notification to Class members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways.

62. Despite the prevalence of public announcements of data breach and data security compromises, the risks posed by compromises of PII, and its own history of security breaches, Defendant failed to take proper action to protect the PII of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measure for its customers.

E. Defendant Has a Duty and Obligation to Protect PII

63. Defendant has an obligation to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII. Defendant's obligations are derived from: 1) government regulations and state laws, including FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided—and Defendant obtained—their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

64. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[39] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification

[39] 17 C.F.R. § 248.201.

number."

65. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices, explaining that the need for data security should be factored into all business decision-making.[40]

66. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for businesses.[41] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[42] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[43] Defendant clearly failed to do any of the foregoing, as evidenced by the Data Breach and amount of data accessed.

67. Here, at all relevant times, Defendant was fully aware of its obligation to protect the PII of its current and former customers including Plaintiff and the Class. Defendant is a sophisticated, multi-billion-dollar, publicly-traded telecommunications services company that

[40] *See* Start with Security, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[41] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[42] *Id*.

[43] *Id*.

relies extensively on technology systems to operate its business, including transmitting its customers' PII over those systems.

68. Defendant had, and continues to have, a duty to exercise reasonable care in collecting, storing, and protecting PII from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiff and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cybersecurity network to secure and protect Plaintiff's and Class members' PII.

69. Defendant's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

70. Further, Defendant had a duty to promptly notify Plaintiff and the Class that their PII was accessed by unauthorized persons.

F. Defendant's Conduct Violated the FTC Act & Industry Standards for Safeguarding Customers' PII

71. The FTC rules, regulations, and guidelines obligate businesses to protect PII from unauthorized access or disclosure by unauthorized persons.

72. At all relevant times, Defendant was fully aware of its obligation to protect its customers' PII because it is a sophisticated business entity that is in the business of maintaining and transmitting PII.

73. Defendant was also aware of the significant consequences of its failure to protect the PII of its customers and knew that this data, if hacked, would injure individuals, including Plaintiff and Class members.

74. Defendant failed to comply with FTC rules, regulations, and guidelines and

industry standards concerning the protection and security of PII. As evidenced by the unknown duration, large scope, and nature of the Data Breach, among its many deficient practices, Defendant failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of current and former customers' PII;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its current and former customers' PII;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures, and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its current and former customers' PII.

75. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers

accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former customers of Defendant would have been notified sooner, allowing them to promptly take protective and mitigating actions.

G. Defendant's Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations

76. Defendant purports to care about data security and safeguarding customers' PII and represents that it will keep secure and confidential the PII belonging to its current and former customers.

77. Plaintiff's and Class members' PII was provided to Defendant in reliance on its promises and self-imposed obligations to keep PII confidential and to secure the PII from unauthorized access by malevolent actors. Defendant failed to do so.

78. Had Defendant undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Defendant would have thwarted hackers' access to its systems in the first instance or otherwise detected the Data Breach prior to the hackers accessing data from Defendant's networks, and Defendant's current and former customers would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

79. Indeed, following the Data Breach, Defendant effectively conceded that its security practices were inadequate and ineffective. In the initial email notice it sent to Plaintiff and others, Defendant acknowledged that the Data Breach required it to hire "external cybersecurity experts to further investigate the incident."[44]

[44] *See* Ex. A.

80. Narayana Pappu, CEO at Zendata, a data protection company, said in a statement that "AT&T should evaluate the processes they have in place to identify exposure and remediation."[45]

81. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[46]

82. The FTC warns the public to pay particular attention to how they keep personally identifying information, including Social Security protection measures and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[47]

83. According to data security experts, one out of every three data breach notification recipients becomes a victim of identity fraud.[48]

84. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

---

[45] https://www.scmagazine.com/news/att-confirms-theft-of-73m-records-7-6m-current-customers-affected (last accessed April 9, 2024).

[46] Roger Cheng, *Data breach hits roughly 15M T-Mobile customers, applicants*, CNET (Oct. 1, 2015).

[47] *Warning Signs of Identity Theft*, Federal Trade Commission, *available at* https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed April 10, 2024).

[48] *A New Identity Fraud Victim Every Two Seconds in 2013 According to Latest Javelin Strategy & Research Study*, Javelin Strategy & Research (Feb. 5, 2014), *available at* https://javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy.

85. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[49] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[50] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has yet to be exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class members' PII will do so at a later date or re-sell it.

86. In response to the Data Breach, Defendant offered to provide certain individuals whose PII was exposed in the Data Breach with one year of credit monitoring. However, one year of complimentary credit monitoring cannot adequately protect against the lifelong risk of harm imposed on Plaintiff and Class members by Defendant's failures.

87. Moreover, the credit monitoring offered by Defendant is inadequate to protect Plaintiff and Class members from the injuries resulting from the unauthorized access of their sensitive PII.

88. Due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and

[49] Susan Ladika, *Study: Data Breaches Pose a Greater Risk*, Fox Business (July 28, 2014), *available at* https://www.foxbusiness.com/features/study-data-breaches-pose-a-greater-risk.

[50] Al Pascual, *The Consumer Data Insecurity Report*, Javelin Strategy & Research (June 30, 2014), *available at* https://javelinstrategy.com/research/consumer-data-insecurity-report.

unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to, lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all these issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

89. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII being accessed by cybercriminals, risks that will not abate within a mere year: the unauthorized access of Plaintiff's and Class members' PII, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendant offered victims of the Breach. The year of credit monitoring that

Defendant offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class members have suffered and will continue to suffer as a result of the Data Breach.

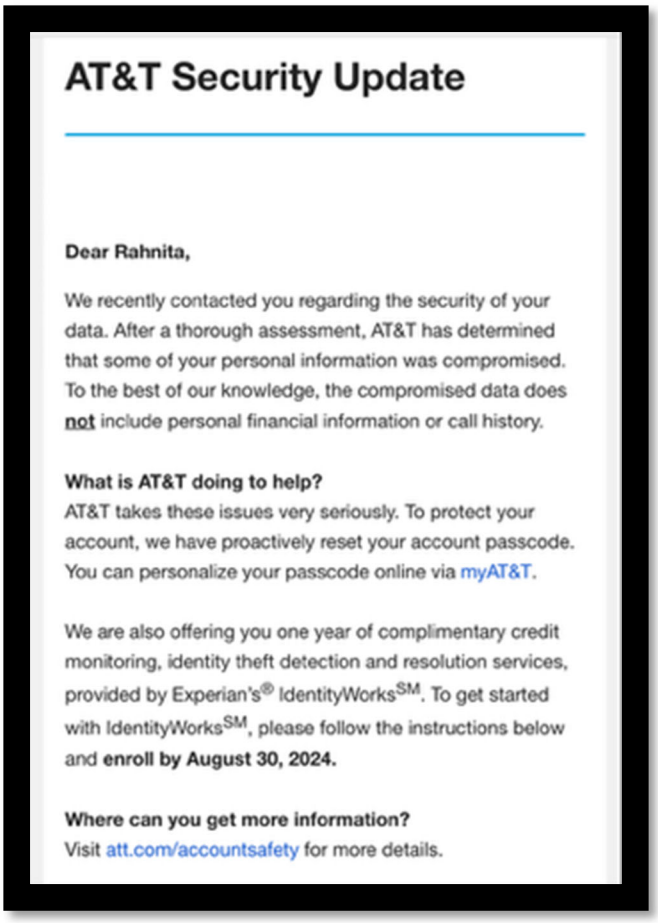
90. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure PII, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft and have incurred and will incur actual damages in an attempt to prevent identity theft.

91. Plaintiff retains an interest in ensuring there are no future breaches, especially given Defendant suffered separate data breach events as recently as January and May 2023, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of herself and similarly situated individuals whose PII was accessed in the Data Breach.

H. Plaintiff's Experience

92. In early April 2024, Plaintiff received a notice from Defendant that her PII had been compromised in the Data Breach and improperly obtained by third parties. The notice indicated that Plaintiff's PII, including her name, phone number, email address, postal address, date of birth, and Social Security number may have been compromised in the Data Breach. Additionally, as a result of the breach, Defendant was required to reset Plaintiff's account passcode. *See* Notice attached as Exhibit A.

93. Shortly thereafter, Plaintiff received an email from Defendant offering her one year of credit monitoring services.



AT&T Security Update

Dear Rahnita,

We recently contacted you regarding the security of your data. After a thorough assessment, AT&T has determined that some of your personal information was compromised. To the best of our knowledge, the compromised data does **not** include personal financial information or call history.

What is AT&T doing to help?
AT&T takes these issues very seriously. To protect your account, we have proactively reset your account passcode. You can personalize your passcode online via myAT&T.

We are also offering you one year of complimentary credit monitoring, identity theft detection and resolution services, provided by Experian's® IdentityWorks℠. To get started with IdentityWorks℠, please follow the instructions below and **enroll by August 30, 2024.**

Where can you get more information?
Visit att.com/accountsafety for more details.

94. As a result of the Data Breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; locking down her accounts and credit; and taking other steps to protect against the use of her PII. Plaintiff has spent valuable time dealing with the Data Breach, time Plaintiff otherwise would have spent on other activities, including work and/or recreation.

95. Plaintiff suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff; (b) violation of her privacy rights; (c) present, imminent, and impending injury arising from the increased risk of identity theft; and

(d) loss of benefit of the bargain.

96. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach, including the short-term loan application that was opened in her name. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

97. Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Nationwide Class defined as:

> **All persons in the United States whose PII was accessed in the Data Breach announced by Defendant on March 30, 2024 (the "Nationwide Class").**

98. Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the Class definition after conducting discovery.

99. In addition, Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), an Illinois Subclass defined as:

> **All persons who are residents of the State of Illinois whose PII was accessed in the Data Breach announced by Defendant on March 30, 2024 (the "Illinois Subclass").**

100. Excluded from the Illinois Subclass are Defendant, its executives and officers, and the Judge(s) assigned to this case.

101. The Nationwide Class and the Illinois Subclass are collectively referred to herein as the "Class."

102. **Numerosity**: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the

Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that at least 73 million individuals were affected by the Data Breach. The members of the Class will be identified through information and records in Defendant's possession, custody, and control.

103. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendant's data security and retention policies were unreasonable;

b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;

d. Whether Defendant breached any legal duties in connection with the Data Breach;

e. Whether Defendant's conduct was intentional, reckless, willful, or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;

g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct;

i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief, and/or other remedies and, if so, the nature of any such relief.

104. **Typicality**: Plaintiff's claims are typical of the claims of the Class because Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The actions and omissions that gave rise to Plaintiff's claims are the same that gave rise to the claims of every other Class member because Plaintiff and each Class member had their sensitive PII compromised in the Data Breach due to Defendant's misconduct, and there are no defenses that are unique to Plaintiff.

105. **Adequacy**: Plaintiff is an adequate representative because her interests do not conflict with the interests of the Class that she seeks to represent, she has retained counsel competent and highly experienced in complex class action litigation, and she intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel.

106. **Superiority**: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of

single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based on Defendant's records.

107. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE

(On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

109. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Defendant collected.

110. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Defendant collected.

111. Defendant owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

112. Defendant owed a duty of care to Plaintiff and the Class because it was a foreseeable and probable victim of any inadequate data security practices.

113. Defendant solicited, gathered, and stored the PII belonging to Plaintiff and the Class.

114. Defendant knew or should have known it inadequately safeguarded this information.

115. Defendant knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and Class members, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

116. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' highly sensitive PII was entrusted to Defendant on the understanding that adequate security precautions would be taken to protect the PII. Moreover, only Defendant had the ability to protect its systems and the PII stored on them from attack.

117. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII. Defendant's misconduct included failing to: (1) secure its systems, servers, and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement safeguards, policies, and procedures necessary to prevent this type of data breach.

118. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiff and the Class.

119. Defendant breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

120. Defendant breached the duties it owed to Plaintiff and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

121. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse

consequences, and thwart future misuse of their PII.

122. Defendant breached the duties it owed to Plaintiff and the Class by failing to disclose timely and accurately to Plaintiff and Class members that their PII had been improperly acquired or accessed.

123. Defendant breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until on or about March 30, 2024.

124. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to, time and expenses incurred in mitigating the effects of the Data Breach.

125. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – NEGLIGENCE *PER SE*

(On Behalf of Plaintiff and the Class)

126. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

127. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

128. The Illinois Consumer Fraud and Deceptive Business Practices Act ("Illinois Consumer Fraud Act"), 815 ILCS 505/1 *et seq*., prohibits unfair or deceptive acts or practices in the conduct of trade or commerce.

129. In addition to the FTC rules and regulations, the Illinois Consumer Fraud Act, and regulations and laws of other states and jurisdictions where victims of the Data Breach are located, require that Defendant protects PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

130. Defendant violated the Illinois Consumer Fraud Act and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards, and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of the Data Breach, and the exposure of Plaintiff's and Class members' sensitive PII.

131. Defendant's violations of the Illinois Consumer Fraud Act, FTC rules, and other applicable statutes, rules, and regulations constitute negligence *per se*.

132. Plaintiff and the Class are within the category of persons the Illinois Consumer Fraud Act and the FTC Act were intended to protect.

133. The harm that occurred as a result of the Data Breach described herein is the type of harm the Illinois Consumer Fraud Act and the FTC Act were intended to guard against.

134. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III - BREACH OF CONTRACT

(On Behalf of Plaintiff and the Class)

135. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

136. Plaintiff and Class members entered into a valid and enforceable contract through which they were required to provide their PII to Defendant in exchange for services.

137. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class members' sensitive personal information to any third parties without their consent.

138. Defendant's promises and Plaintiff's and Class Members' rights and obligations are memorialized in AT&T's privacy policy, published on its website. Defendant's privacy policy is part of Plaintiff's and Class Members' agreement for services with AT&T.

139. Plaintiff and Class Members fully performed their obligations pursuant to their contracts with AT&T. Defendant breached its contracts with Plaintiff and Class Members when it failed to protect, secure, and/or keep private Plaintiff's and Class Members' PII.

140. As a result, Plaintiff and Class members have been harmed, damaged, and/or injured as described herein, including by Defendant's failure to fully perform its part of the agreement with Plaintiff and Class members.

141. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV - BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Class)

142. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

143. When Plaintiff and Class Members provided their PII to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiff's and Class Members' PII, comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII, and to timely notify them in the event of a data breach.

144. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's provision of cellular services. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

145. Implicit in the agreement between Plaintiff and Class Members and Defendant was Defendant's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard Plaintiff's and Class Members' PII; (c) prevent unauthorized access and/or disclosure of Plaintiff's and Class Members' PII; (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or disclosure of their PII; (e) reasonably safeguard and protect the PII of Plaintiff's and Class Members from unauthorized access and/or disclosure; and (f) retain Plaintiff's and Class Members' PII under conditions that kept such information secure and confidential.

146. Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

147. Plaintiff and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

148. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

149. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard their PII and by failing to provide them with timely and accurate notice of the Data Breach.

150. The losses and damages Plaintiff and Class Members sustained, include, but are not

limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members'

data;

i. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members;

j. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class Members.

COUNT V - VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT (CONSUMER FRAUD ACT) (815 ILLINOIS COMPILED STATUTES 505/1 et seq.)

(On Behalf of Plaintiff and the Illinois Subclass)

151. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

152. The Illinois Consumer Fraud and Deceptive Business Practices Act ("Illinois Consumer Fraud Act"), 815 ILCS 505/1 et seq. declares unlawful "any . . . false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, . . . in the conduct of any trade or commerce . . . whether any person has in fact been misled, deceived or damaged thereby."

153. Plaintiff and other members of the Illinois Subclass are "persons" within the meaning of 815 ILCS 505/1 § (1)(b).

154. Defendant's conduct alleged herein constitutes a "sale" within the meaning of 815 ILCS 505/1 § (1)(d) because Plaintiff and the Class's data is now offered for sale on the dark web.

155. In the Privacy Policy, Defendant represented to Plaintiff and the Class Members that their PII would be protected and/or securely maintained by virtue of security programs and information technology security measures.

156. By requiring Plaintiff and Class Members to agree to Defendant's Privacy Policy, Defendant intended Plaintiff and the Class Members to rely on it. The Privacy Policy represented that Plaintiff's and Class Members' PII would be protected by Defendant. Plaintiff and Class Members were required to agree to Defendant's Privacy Policy in order to apply for or use Defendant's services. Plaintiff and Class Members relied on Defendant to protect and/or secure their PII per the Privacy Policy.

157. Defendant's misrepresentations and false, deceptive, and misleading statements and omissions with respect to its privacy policy as described above, constitute affirmative misrepresentations in violation of the Illinois Consumer Fraud Act.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court enter a judgment on their behalf and against Defendant AT&T, Inc., and further grant the following relief:

A. Certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure;

B. Designate Plaintiff as a representative of the proposed Class and subclass and Plaintiff's counsel as Class counsel;

C. Grant Plaintiff the declaratory relief sought herein;

D. Grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

E. Award Plaintiff and the Class compensatory, consequential, and general damages in an amount to be determined at trial, and any other relief to which they are entitled under the law;

F. Award Plaintiff and the Class statutory damages, and punitive or exemplary damages, to the extent permitted by law;

G. Award prejudgment interest, costs, and attorneys' fees;

H. Award all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. Award Plaintiff and the Class such other and further relief as the Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the proposed Class, respectfully requests a trial by jury as to all matters so triable.

Dated: April 12, 2024

Respectfully submitted,

By: */s/ Elizabeth A. Fegan*

Elizabeth A. Fegan
Megan E. Shannon
FEGAN SCOTT LLC
150 S. Wacker Drive, 24th Floor
Chicago, IL 60606
Telephone: (312) 741-1019
Facsimile: (312) 264-0100
beth@feganscott.com
megan@feganscott.com